民間網路戰士：我國可運用途徑

曾怡碩

網路作戰與資訊安全研究所

壹、前言

資通電軍指揮部招募後備網路戰士，進一步運用民間網路專長，引發各界側目。鑒於網路戰場無分前後方與無國界特性，除須採取全社會取向（whole-of-society approach）的網路防衛，且許多擅長網路作戰的高手在民間，故勢必設法讓民間網路作戰能量能夠適時發揮。但民間網戰能量的呼應與發揮，除了大家熟知的網路駭客以及前述後備役資訊資安專長人士，還能如何運用？不同運用途徑對台灣又產生哪些機會與啟示？

由前述網路戰特質，可理解需動用民間之人力專長包括網路攻擊、網路實體設施維運與網路訊息製作傳播，本文主要以網路攻擊與資安專長為探討對象。此外，由於網路戰仍屬新興領域，網路司令部在多國均屬新的嘗試，對於如何運用後備及民力支援或補充網路作戰，更是尚待發展精進的領域，相關探討可參見本期特刊杜貞儀博士專文。本篇則藉由軍文關係研究中關於組成構面的來源、戰力、信念，以及民主監督控制構面的法治與政治控制，探討兩大類民間戰士身分特質與市場因素：後備戰士（含後備役、公民戰士、民兵)以及雇用關係（含傭兵)。除從中釐清辨識各自所產生的機會與風險，並藉此檢視台灣運用現況與建議未來可行方案。

貳、民間網路戰士：身分特質與市場因素

網路戰是新型態戰爭，藉虛擬網路空間與實體設備施行滲透、監測、破壞與影響力作戰，具有以下特質：其一、網路無國界，讓網路戰場無前後方與國內外之分野。其二、不論是網路攻擊還是散布假訊

息之資訊作戰，往往難以藉由網路空間溯源辨識與確認攻擊來源，且造成之破壞後果未達傳統實體空間武裝衝突傷亡或損壞程度，維持在戰爭門檻之下，故具灰色地帶衝突特性。其三、運用網路互相連結之特性，網路戰可成為小國制衡大國的不對稱作戰利器，網路戰的勝負並非取決於投入戰場人數的數量，而是以質量取勝，故民間高手的效力極可能成為扭轉戰局的關鍵。同理亦可證諸於網路戰的防禦，由於網路相互連結，唯有全社會取向之防禦足以形成重層防衛。上述這些網路戰場特質，是讓民間網路戰士角色吃重的原因，未必能在其他樣態戰場套用。

一、後備戰士

（一)後備役

後備役一般是徵兵制或募兵制國家於戰時或必要時機，動員投入以補充現役兵員，藉此控制現役專業軍隊規模，並兼顧經濟民生之發展。後備役的規模、對其訓練質量與動員能力，均足以納入對該國軍力之評估，並形成一國之嚇阻力量。一般後備役即為義務役，或自願役軍人退伍後一定時間內，在教點召時受訓，以維繫戰力及保家衛國信念。其受訓與動員均受民主法治監督與管制，必要時得以後備教點召兵員投入平日國家所需，例如防救災後備戰士、資安後備戰士、防疫國家隊等，在緊急或必要時刻則動員投入保家衛民。

在網路戰場迫切需要專才投入的狀況下，循國家後備體制，將具資安網戰專長之後備役納入資安後備戰士註記、訓練，已是諸如我國、以色列、美國以及愛沙尼亞等網路資安領域先進國家所採取之途徑。由於不缺乏實際練兵的場域，資安後備戰士如能充分運用，將形成可觀戰力。

（二)公民戰士

新加坡與瑞士的全部男性、以色列的全體公民均需服役，退伍後成為後備役，這樣全民皆兵的體制下之兵員，即為公民戰士。公民戰士其實可追溯至古希臘時代，雅典與斯巴達之公民同時也是戰士。公民戰士可以藉軍事訓練與保家衛國，讓公民更加認同國家，戰力也隨之加強，往往形成對外敵的嚇阻力量。另一方面，全民皆兵是相對於專業軍隊的另一端，全民均可成為防衛力量，以避免武力集中軍隊而導致軍事政變之風險。然而，大規模公民服役也可能因此造就軍事化的社會氛圍，進而限縮並危及公民權利。[1]

將公民戰士應用於網路戰場，類似於後備役之狀況，只是須注意人才專長之動態變化，須納編原服役期間未具資安網路專長、但後備役期間投入該領域而後具備此項專長者。如果一國存在完整的網路資安產業生態系統，不僅源源不絕的網路公民戰士讓該國具備可恃之網戰能量，也能帶動產業持續創新增長。最著名的例子就是全民皆兵的以色列，經過長年經營，已是全球資安產業領域的大國。

(三)民兵

相對於公民戰士，民兵是為較常見之型態。民兵的特質在於有限度自願性投入、地方召募與服役、有限度投入戰鬥。[2]一般所稱民防、敵後游擊隊，或耳熟能詳的美國國民兵、我國之金馬自衛隊、中共在東海與南海所部署的海上民兵，均屬此類性質。另一方面，關於全球各地內戰的資訊，民兵組織亦常被提及。在俄羅斯入侵克里米亞的混合戰中，民兵也在灰色地帶衝突中扮演重要角色。民兵來源成分多元，其地域特性使其未必受國家直接指揮，且訓練強度不一，戰力水準也參差不齊。

---

[1] Eliot Cohen, *Citizens and Soldiers*, Cornell University Press, 1985, pp.123-125.
[2] Eliot Cohen, ibid., p. 127.

網路民兵若淪為網路游擊隊，則與黑帽駭客相差無幾，如果與計價報酬掛勾，則淪為網路傭兵。另一方面，網路民兵若有極權國家政府在背後統籌指揮，則規模將相當可觀，可充分運用於對內部控制與對外戰狼征戰。在中國「人民戰爭」的指導下，網路民兵除進行網路戰，主要還是以網路監察與網路涉外論戰為主。[3]然而，中國各地之網監或戰狼五毛黨，實質已經涉及金錢報酬，其實與廉價網路傭兵無異。

二、傭兵與商業合作

（一)傭兵

相對於國家化的政府軍隊，傭兵的性質屬於私有化的武力，而且歷史更為悠久。私有化武力其實也包括效忠於強人的軍閥所屬部隊，但傭兵個別或集體效忠於所簽之合約，一般具有金錢對價關係。有了市場價格因素，高報酬的傭兵所從事多為高風險性質任務。嚴格說來，涉及對價合約的私人武力範疇，包括保全與保鏢，所從事任務的環境，也有可能是在城鎮戰場或海上護航。[4]網路傭兵在近年已在暗網形成新興黑市，網路攻擊或病毒軟體開發駭客個體戶或團隊待價而沽，掮客絡繹不絕，企業、政府之情報與網戰單位均成主顧，形成「政府-企業-駭客」之網路傭兵市場結構。近年來，由特定國家或政府支持之網路進階持續攻擊團隊對於全球網路安全造成相當大的破壞力，由於網路傭兵唯利是圖，無國家忠誠度可言，可能在達成委辦項目之後，伺機自己進一步訛詐掠奪。在新冠肺炎疫情居家上班及更為倚重網路通訊之情形下，諸如傭兵駭客竊取金融機構之金錢與利用勒索軟體索取贖金等事件層出不窮。

---

[3] 王清安，〈中共網軍發展對本軍威脅評估之研究〉，《陸軍通資半年刊》，第 127 期，2017 年 4 月》，頁 14。

[4] Deborah Avant, *The Markets for Forces: The Consequences of Privatizing Security*, Cornell University Press, September, 2005, pp.128 -151

（二)合法商業合作

美國現役的網戰人力在召募與留用方面均面臨挑戰。但美國軍方善於與國防工業企業合作，在網路作戰方面，主要集中在威脅情報分析、通報與分享系統建置、軟硬體採購，及訓練維保。以色列則在網戰人才退伍成為公民後備役時，鼓勵其成立資安新創公司，並與以色列軍方及政府保持商業合作關係，故其資安產業蓬勃發展，也促進年輕網戰專才願意投入以色列網戰部隊效力，從而創造人力運用良性循環的生態系。

鑒於資安與網攻為一體兩面，資安防禦網路攻擊，自然必須了解網路攻擊實務操作。因此，有意運用網路後備戰士的國家，平日加強扶植資安產業，投入資安產業人力增長，則不失為藉由市場因素訓練培育網戰人才的一舉兩得途徑。但首先應須注意人才專長動態，納編原服役期間未具資安網路專長、但後備役期間投入該領域而後具備此項專長者。其次，後備教召時期短暫，除非連續每期教召均有源源不絕的網戰資安專長人士，否則對於持續補充網路戰力幫助仍有限。

參、發展運用民間網路戰士的分析與建議

以下首先針對於運用不同類型的民間網路戰士進行初步利害關係分析，其次再依台灣運作現況，提出相關建議。

一、分析

其一，資網路資安後備戰士能運用專長已註記編管的後備役人員，但是就整體社會而言，一般後備役仍屬於局部動員性質，還存有相當的餘裕與韌性可因應網路威脅，例如可以和不在註記名冊內或非後備役之白帽駭客分進合擊。相對地，網路後備戰士制度的缺失，則在於部隊規模不夠大，且平時高手可能不願現身。

其次，網路傭兵戰力素質最高，且受市場價格驅使，可及性也高，甚至可以雇用外籍網路傭兵，故無來源短缺之虞。另一方面，前述優點卻也因為網路傭兵無忠誠度，今日受雇我方可成助力，明日也可受雇他方而反噬，或為犯我之敵手，或為擾我之恐怖份子。

二、對我國可運用途徑之建議

資通電軍指揮部於 2017 年 7 月 1 日成立，由於人才供需市場結構與薪資因素限制，與其他國家一樣面臨召募與留用問題，旋於 2018 年 1 月 1 日起，開始實施「網路戰士志願短期在營服役」，希望藉鼓勵國軍屆退官兵及提供後備軍人多重服役選擇，以充實網路戰大隊的人力。網路戰士享有待遇、加給、口糧代金及一天有 500 元的網戰勤務加給。「後備戰士」採「每月入營 2 日（以周末為主)、1 次演訓 7 日」之作法定期返營，全年至少在營 29 日。「後備戰士」在營期間(含留宿)具有現役軍人身分，須遵守國家法令及對公務保守機密之責任；離營後恢復後備軍人身分。據該年立法院法制局研究報告指出，該年軍方為這類戰士薪餉僅編列 65 萬元，顯示其招募規模太小且建構之目標亟待加強。[5]時至今日，今（2020)年資通電軍將召募 7 員後備戰士，規模仍不足。[6]

鑒於我國積極提倡資安產業，依前述分析，理應具備相當規模之網路後備戰士，但須先結合專長登記，將原先非該專長，爾後投入資安產業具備網路戰專長人士納入專長註記。此外，由於依「從事國防事務現職及退（離）職人員申請進入大陸地區作業規定」辦理，於服「後備戰士」期間不得赴大陸地區，讓一些企業界從業人士擔心生涯發展受限。對此，建議須對企業與個人均提供誘因，諸如專案合作、

---

[5] 蘇顯星，〈建構「資通電軍」新軍種之配套措施與修法方向研析〉，《立法院法制局議題研析》R00574 號，107 年 11 月 1 日，https://www.ly.gov.tw/Pages/Detail.aspx?nodeid=6590&pid=176016。

[6] 〈國軍 109 年「後備戰士」實施作法問答集〉，國防部後備指揮部，https://afrc.mnd.gov.tw/AFRCWeb/Content.aspx?MenuID=702。

減稅鼓勵、薪資補貼，才能讓企業主不會技術性阻擋具專長部屬投入後備戰士，也才能讓具專長個人願意加入後備戰士隊伍。尤其應鼓勵軍民商業合作，讓後備戰士平日在營服役，因應我國非假日期間高強度之網路威脅，企業主也得到商機與減稅、薪資補助，進一步鼓勵員工加入後備戰士行列，如此可望形成良性正向循環。

肆、結論

網路戰場的特質，讓發展運用民間網路戰士成為理性計算下可行之道，但不同的運用態樣，產生的後果各異，對民主社會而言，在兼顧民主法治與國家發展的前提下，必須對發展運用民間網路戰士的途徑進行評估。本篇研究初步發現，後備網路戰士相對風險最低，若結合民間白帽駭客，戰力將獲大幅提升。基於台灣積極發展資安產業，若能有效結合專長追蹤註記，網路後備戰士的數量將有可觀增長。此外，本文建議結合資安產業商業合作，以商業合作、減稅或補助方式，直接提供誘因給資安企業及後備網路戰士個人，配合我軍面對網供威脅樣態，提升平日期間召集網路後備戰士回營服役之意願，冀能有效結合並運用民間網路作戰能量，以因應來自對岸及各方之高強度網路威脅。

本文作者曾怡碩為美國喬治華盛頓大學政治學博士，現為財團法人國防安全研究院網路作戰與資訊安全研究所所長。

Civil Cyber Warriors: A Path that Taiwan Can Take

Yi-Suo Tzeng,
Assistant Research Fellow

Abstract

The characteristics of the cyber battlefield make developing and using civil cyber warriors a feasible way when logically considered, however, different types of use will produce different consequences. Under the prerequisites of democracy and rule of law and national development, a democratic society must assess the approach of developing and using civil cyber warriors. This paper will discuss the identity characteristics of the two main types of civil warrior and market factors: reserve warriors (including reserve, citizen warriors, and militia) and employment relations (including mercenaries.) Research initially shows that the relative risk of reserve cyber warriors is lowest and if they are combined with civil "white hat" hackers, combat power will be substantially increased. As Taiwan is actively developing the information security industry, the number of cyber reserve warriors can be greatly increased if we can effectively combine with tracking and notation expertise.

In addition, this paper suggests commercial cooperation with the information security industry, using commercial cooperation, tax reduction or subsidy to directly induce information security enterprises and individual reserve cyber warriors to assist Taiwan's military face the various cyber threats and increase the willingness of reserve cyber warriors to return to base to serve at ordinary times, to effectively combine with and utilize civil cyber combat capability in response to the cyber threat from the other side of the Taiwan Strait and others.